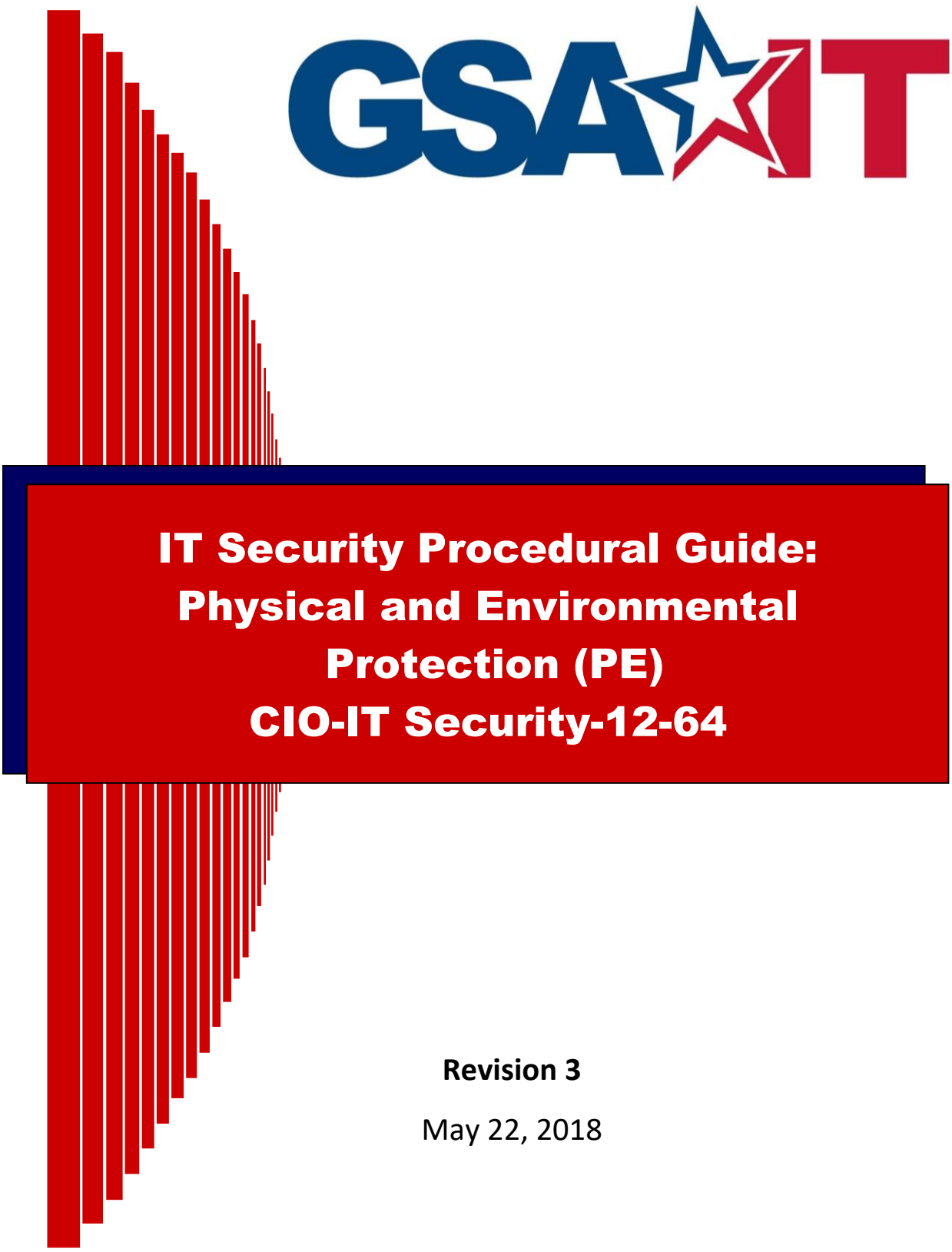


IT Security Procedural Guide: Physical and Environmental Protection (PE) CIO-IT Security-12-64

Revision 3

May 22, 2018

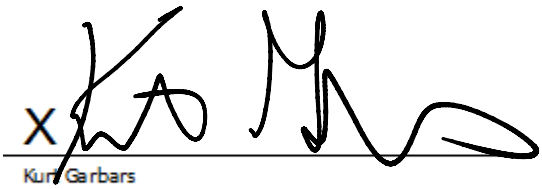
Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 – March 30, 2012				
1	Heard	New product	Provide guidance for NIST 800 53 Rev 4 controls	Various
Revision 2 Changes – May 16, 2016				
1	Sitcharing	Changes made throughout the document to reflect NIST and GSA requirements	Updated to reflect and implement most current NIST 800-53 and GSA requirements	Various
2	Klemens/ Wilson	Changes made throughout the document to reflect Government comments.	Updated to reflect Government comments.	Various
Revision 3 Changes - May 22, 2018				
1	Feliksa/ Klemens	Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework.	Biennial update.	Various

Approval

IT Security Procedural Guide: Physical and Environmental Protection (PE), CIO-IT Security-12-64, Revision 3 is approved for distribution.



Kurt Garbars
Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

1 Introduction 1
1.1 Purpose 2
1.2 Scope 2
1.3 Policy 2
1.4 References 3
2 Roles and Responsibilities 4
2.1 GSA Chief Information Security Officer (CISO) 4
2.2 Authorizing Official (AO) 5
2.3 Information Systems Security Manager (ISSM) 5
2.4 Information Systems Security Officer (ISSO) 5
2.5 System Owners 5
2.6 Data Owners 5
2.7 Custodians 6
2.8 Authorized Users of IT Resources 6
2.9 Supervisors 6
3 GSA Guidance for PE Controls 6
3.1 PE-1 Physical and Environmental Protection Policy and Procedures 7
3.2 PE-2 Physical Access Authorizations 8
3.3 PE-3 Physical Access Control 8
3.4 PE-4 Access Control for Transmission Medium 10
3.5 PE-5 Access Control for Output Devices 10
3.6 PE-6 Monitoring Physical Access 10
3.7 PE-8 Visitor Access Records 11
3.8 PE-9 Power Equipment and Cabling 12
3.9 PE-10 Emergency Shutoff 13
3.10 PE-11 Emergency Power 13
3.11 PE-12 Emergency Lighting 14
3.12 PE-13 Fire Protection 14
3.13 PE-14 Temperature and Humidity Controls 15
3.14 PE-15 Water Damage Protection 15
3.15 PE-16 Delivery and Removal 16
3.16 PE-17 Alternate Work Site 16
3.17 PE-18 Location of Information System Components 17
4 Physical and Environmental Protection and Supply Chain Risk Management 17
4.1 PE-1 Physical and Environmental Protection Policy and Procedures (ICT SCRM) 18
4.2 PE-3 Physical Access Control (ICT SCRM) 18
4.3 PE-6 Monitoring Physical Access (ICT SCRM) 19
4.4 PE-16 Delivery and Removal (ICT SCRM) 19
4.5 PE-17 Alternate Work Site (ICT SCRM) 20
4.6 PE-18 Location of Information System Components (ICT SCRM) 20
5 Summary 20

Table 1-1: NIST SP 800-53 Control to CSF Mapping 2

1 Introduction

Physical and environmental protection (PE) focuses on physically securing an Information Technology (IT) information system and its components in its operational environment. This guide provides guidance for mitigating the risks from physical and environmental threats through the implementation of NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*" PE controls. Implementation of these controls help GSA protect IT Security Assets from physical and environmental threats.

Every General Services Administration (GSA) IT system must follow the PE practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*" must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form. Deviations must also be documented using the Acceptance of Risk (AoR) process defined in GSA CIO-IT Security-06-30, "*Managing Enterprise Risk"*, including a date of resolution to comply.

Executive Order (EO) 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*" requires all agencies to use "*The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology (NIST) or any successor document to manage the agency's cybersecurity risk.*" This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework from NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach.*" Table 1-1 provides a mapping of the NIST SP 800-53 PE controls to CSF Category Unique Identifiers. The following CSF categories/subcategories are aligned with NIST's PE controls.

- **Identify:** Business Environment (ID.BE), Governance (ID.GV)
- **Protect:** Identity Management and Access Control (PR.AC), Data Security (PR.DS), Information Protection Processes and Procedures (PR.IP)
- **Detect:** Security Continuous Monitoring (DE.CM), Detection Processes (DE.DP)
- **Respond:** Analysis (RS.AN), Communications (RS.CO)

Table 1-1: NIST SP 800-53 Control to CSF Mapping

NIST 800-53 Control	CSF Category Unique Identifier Codes	NIST 800-53 Control	CSF Category Unique Identifier Codes
PE-1	ID.GV-1, ID.GV-3	PE-11	ID.BE-4
PE-2	PR.AC-2, PR.AC-6	PE-12	PR.IP-5
PE-3	PR.AC-2, DE.CM-2, DE.CM-7, DE.DP-3	PE-13	PR.IP-5
PE-4	PR.AC-2	PE-14	PR.IP-5
PE-5	PR.AC-2	PE-15	PR.IP-5
PE-6	PR.AC-2, DE.CM-2, DE.CM-7, RS.CO-3, RS.AN-1	PE-16	PR.DS-3
PE-8	PR.AC-2	PE-17	PR.IP-9
PE-9	ID.BE-4	PE-18	PR.IP-5
PE-10	PR.IP-5		

1.1 Purpose

The purpose of this guide is to provide guidance for the PE security controls identified in NIST SP 800-53 and physical and environmental requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in CIO 2100.1, and other IT personnel involved in the physical and environmental protection of IT assets the specific procedures and processes they are to follow for protecting GSA information systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to, and must be followed, by all GSA Federal employees and contractors involved in providing physical and environmental protection for GSA information systems and data. Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

1.3 Policy

PE is covered in Chapter 4, paragraph 2 of CIO 2100.1 as stated below.

b. Physical and environmental protections.

(1) Physical and environmntal security controls must be commensurate with the level of risk and must be sufficient to safeguard IT resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

(2) GSA servers, routers, and other communication hardware essential for maintaining the operability of GSA systems and their connectivity to the GSA Network, must be placed in an isolated, controlled-access location (i.e., behind locked doors).

(3) Limit access to rooms, work areas/spaces, and facilities that contain agency systems, networks, and data to authorized personnel. A list of current personnel with authorized

access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

(4) Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). Visitor access records include: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; (vii) name and organization of person visited, and (viii) signature and name of individual verifying the visitor's credentials. Visitor access records shall be reviewed at least annually.

(5) Ensure that all agency systems and networks are located in areas not in danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment to support meeting federal and local building codes.

(6) Install and ensure operability of fire suppression devices, such as fire extinguishers and sprinkler systems, and detection devices, such as smoke and water detectors, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

(7) Install and ensure operability of air control devices, such as air-conditioners and humidity controls, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

(8) Ensure that guidance provided in the GSA CIO-IT Security-12-64: Physical and Environmental Protection for a secure environment for information systems, including physical access control, fire protection, emergency power, and alternate sites are implemented. Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

1.4 References

Note: GSA updates its IT security policies and procedural guides on independent biennial cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws and Regulations:

- EO 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*"
- HSPD 12, "*Policy for a Common Identification Standard for Federal Employees and Contractors*"

Federal Guidance:

- CSF, "*Framework for Improving Critical Infrastructure Cybersecurity*"
- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"

- NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-161, "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*"

GSA Guidance:

- GSA Order ADM CIO 2450.1, "*Alternate Sites for Continuity of Operations Plan (COOP) Relocation*"
- GSA Order ADM 5900.1, "*Physical Access Control Systems in U.S. General Services Administration Controlled Space*"
- GSA Order ADM P 9732.1D, "*Suitability and Personnel Security"*
- GSA Order HCO 6040.1A, "*GSA Mobility and Telework Policy*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2104.1A, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order CIO 2182.2, *"Mandatory Use of Personal Identity Verification (PIV) Credentials"*

The documents below are available on the GSA IT Security Procedural Guides InSite page.

- CIO-IT Security-01-02, "*Incident Response (IR)*"
- CIO-IT Security-01-05, "*Configuration Management*"
- CIO-IT Security-01-07, "*Access Control (AC)*"
- CIO-IT Security-03-23, "*Termination and Transfer*"
- CIO-IT Security-18-90, "*Information Security Program Plan*"

2 Roles and Responsibilities

There are many roles associated with implementing effective physical and environmental protection for IT systems. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. Throughout this guide, specific processes and procedures for implementing NIST's PE controls are described.

2.1 GSA Chief Information Security Officer (CISO)

Responsibilities include the following:

- Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with this policy.
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.

2.2 Authorizing Official (AO)

Responsibilities include the following:

- Establishing physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

2.3 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Coordinating with ISSOs to establish and manage processes and procedures supporting PE controls for all systems under their purview.
- Monitoring and supporting the resolution of POA&Ms to mitigate system vulnerabilities for all systems under their purview.
- Ensuring GSA IT security policies and procedures are followed.

2.4 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary PE security controls are in place and operating as intended.
- Developing POA&Ms, when necessary, for all systems under their purview.
- Ensuring media handling procedures are followed.

2.5 System Owners

Responsibilities include the following:

- Ensuring necessary PE controls are in place and operating as intended.
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems.
- Ensuring that physical or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk.

2.6 Data Owners

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA.
- Ensuring protection of GSA's systems and data IAW GSA's IT Security Policy and the GSA Records Management Program.
- Coordinating with IT security personnel including the ISSM and ISSO and system owners to ensure implementation of system and data security requirements.

2.7 Custodians

Responsibilities include the following:

- Coordinating with Data Owners and System Owners to ensure the data is properly stored, maintained, and protected.
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO.
- Providing the OCISO physical access to devices when needed as part of any incident response effort.

2.8 Authorized Users of IT Resources

Responsibilities include the following:

- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data.
- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver before leaving their workstation.

2.9 Supervisors

Responsibilities include the following:

- Coordinating and arranging system access requests for all new or transferring employees and for verifying an individual's business 'need-to-know' (authorization).
- Coordinating and arranging system access termination for all departing or resigning personnel.
- Coordinating and arranging system access modifications for personnel.

3 GSA Guidance for PE Controls

The GSA-defined parameter settings included in the control requirements are offset by brackets in the control text. As stated in Section 1.2, the requirements outlined within this guide apply to and must be followed by all GSA Federal Employees, contractors and employees of GSA who are involved in providing physical and environmental protection for GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions/requirements for contractor systems will be included in the "Additional Contractor System Considerations" portion of each control section.

PE-1, Physical and Environmental Protection Policy and Procedures, has been identified as a Common Control for all GSA/internally operated systems by GSA and as a Hybrid Control for contractor systems. The PE-2 to PE-18 controls, when included in a system's control set, either

are provided as a Common Control by a Major Information System, a system specific control by the system, or as a Hybrid Control with shared responsibilities for control implementation. CIO-IT Security-18-90, "*Information Security Program Plan*" describes the GSA enterprise-wide inheritable common and hybrid controls and outlines the responsible party for implementing each of them.

3.1 PE-1 Physical and Environmental Protection Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to [*Information System Security Manager, Information System Security Officer, System Owners, Acquisitions/Contracting Officers, Custodians*]:
    1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
b. Reviews and updates the current:
    1. Physical and environmental protection policy [*biennially*]; and
    2. Physical and environmental protection procedures [*biennially*].

GSA Implementation Guidance: Control PE-1 is applicable at all FIPS 199 levels.

Physical and environmental protection policy and procedures is a common control provided by the GSA OCISO Policy and Compliance Division (ISP). Physical and environmental protection policy is included in CIO 2100.1, Chapter 4, Policy on Operational Controls. The policy states: "*Physical and environmental security controls must be commensurate with the level of risk and must be sufficient to safeguard IT resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.*" GSA OCISO ISP also defined agency-wide access control procedures in CIO-IT Security-01-07, "*Access Control (AC).*"

GSA Service/Staff Office (S/SO) organizations are encouraged to have separate PE policies and procedures to supplement CIO 2100.1 and this guide. Supplemental procedures must be unique to the S/SO, system, data type (financial, privacy, etc.) and convey the organization's implementation of common and/or hybrid controls as defined in the current version of NIST SP 800-37.

CIO 2100.1 and this guide are reviewed and updated at least biennially.

Additional Contractor System Considerations:

Vendors/contractors may defer to the GSA policy and guide or implement their own physical and environmental protection policies and procedures which comply with GSA's requirements with the approval of the Authorizing Official (AO).

3.2 PE-2 Physical Access Authorizations

Control: The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals [*at least annually*]; and
d. Removes individuals from the facility access list when access is no longer required.

GSA Implementation Guidance: Control PE-2 is applicable at all FIPS 199 levels.

GSA requires a current list of personnel and roles authorized physical access to the system to be maintained along with the appropriate System Security Plan (SSP). GSA requires the acceptance of Federal Personal Identity Verification (PIV) smartcard credentials as the common means to authenticate federal employee and contractor access to the GSA facilities, networks, and information systems IAW GSA Order CIO 2182.2*, "Mandatory Use of Personal Identity Verification (PIV) Credentials*". The facility access list should be updated and reviewed at least annually. Individuals no longer requiring access should be removed IAW CIO-IT Security-03-23, "*Termination and Transfer.*"

This control only applies to areas within facilities that have not been designated as publicly accessible. Due to the sensitive nature of information stored within GSA facilities, it is important that individuals lacking sufficient security clearances, access approvals, or a business 'need-to-know,' be escorted by individuals with appropriate credentials to ensure that such information is not exposed or otherwise compromised.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.3 PE-3 Physical Access Control

Control: The organization:

a. Enforces physical access authorizations at [*GSA S/SO or Contractor recommended and AO approved entry/exit points to the facility where the information system resides*] by;
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress/egress to the facility using [*Physical Access Control Systems (PACS) devices IAW GSA Order ADM 5900.1, and guards for on-premises contracts; S/SO or Contractor recommended and GSA AO approved physical access control systems, devices, guards for off-premises contracts*];
b. Maintains physical access audit logs for [*GSA S/SO or Contractor recommended entry/exit points approved by the AO*];
c. Provides [*GSA S/SO or Contractor recommended security safeguards approved by the AO*] to control access to areas within the facility officially designated as publicly accessible;

d. Escorts visitors and monitors visitor activity [*GSA S/SO or Contractor recommended circumstances requiring visitor escorts and monitoring approved by the GSA AO*];
e. Secures keys, combinations, and other physical access devices;
f. Inventories [GSA *S/SO or Contractor recommended physical access devices approved by the AO*] every [*year*]; and
g. Changes combinations and keys [*at least annually*] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Control Enhancements:

(1) Physical Access Control | Information System Access. The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [*GSA S/SO or Contractor recommended and AO approved physical spaces containing one or more components of the information system*].

GSA Implementation Guidance: Control PE-3 is applicable at all FIPS 199 levels. Enhancement PE-3(1) is applicable at the FIPS 199 High level.

GSA authorizes facility access prior to granting access to information systems. GSA requires mandatory use of PIV credentials for individual access to GSA facilities IAW CIO 2182.2. Additionally, GSA has established an agency-wide approach and policy to update, procure, and install HSPD-12 compliant Physical Access Control Systems (PACS) in GSA controlled space(s) IAW GSA Order ADM 5900.1, "*Physical Access Control Systems in U.S. General Services Administration Controlled Space*." Ingress/egress to information systems in non-GSA facilities must be controlled using GSA AO approved physical access control systems, devices, guards.

Physical access audit logs must be maintained at the GSA facility in which the information system resides and reviewed IAW PE-6. Audit logs can be procedural (e.g., a written log of individuals accessing the GSA facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include GSA facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. When escorts are required, the escort must be identified in the visitor access record IAW PE-8.

Keys, combinations, and other physical access devices must be secured (as necessary), and changed annually. Inventories of physical access devices must be approved, at least annually by the AO.

For enhancement PE-3(1), FIPS 199 High impact systems must require physical access authorizations and restrict access to GSA AO approved physical areas containing the system or any of its components.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.4 PE-4 Access Control for Transmission Medium

Control: The organization controls physical access to [*GSA S/SO or Contractor recommended and AO approved information system distribution and transmission lines*] within organizational facilities using [*GSA S/SO or Contractor recommended and AO approved security safeguards*].

GSA Implementation Guidance: Control PE-4 is applicable at the FIPS 199 Moderate and High level.

This control ensures that GSA and its custodians protect against accidental or intentional damage or disruption of distribution and transmission lines located within facilities housing GSA information systems. In addition, physical safeguards may be necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Adequate protections include but are not limited to locked wiring closets, use of protective cable conduit or trays, and disconnecting or locking spare jacks.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.5 PE-5 Access Control for Output Devices

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

GSA Implementation Guidance: Control PE-5 is applicable at the FIPS 199 Moderate and High level.

GSA protects against physical access to information by unauthorized individuals. Examples of output devices are monitors, printers, and audio devices. Protective methods include locating output devices within controlled access areas, separate from areas designated publically accessible.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.6 PE-6 Monitoring Physical Access

Control: The organization:

a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
b. Reviews physical access logs [*at least annually*] and upon occurrence of [*physical security incidents*]; and
c. Coordinates results of reviews and investigations with the organizational incident response capability.

Control Enhancements:

(1) Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment. The organization monitors physical intrusion alarms and surveillance equipment.

(4) Monitoring Physical Access | Monitoring Physical Access to Information Systems. The organization monitors physical access to the information system in addition to the physical access monitoring of the facility at [*GSA S/SO or Contractor recommended and AO approved physical spaces containing one or more components of the information system*].

GSA Implementation Guidance: Control PE-6 is applicable at all FIPS 199 levels. Enhancement PE-6(1) is applicable at the FIPS 199 Moderate and High level. Enhancement PE-6(4) is applicable at the FIPS 199 High level.

GSA monitors access to physical spaces containing one or more components of GSA information systems in addition to the physical access monitoring of the facility to detect and respond to unauthorized access as well as to support the investigation of security incidents. All GSA incident response activities are handled in agreement with CIO-IT Security-01-02, "*Incident Response (IR)*."

GSA reviews physical access logs at least annually. GSA coordinates reviews, which may indicate unauthorized access, or results from investigations through GSA's incident response staff per CIO-IT Security-01-02.

For enhancement PE-6(1), FIPS 199 Moderate and High Impact systems must provide physical intrusion alarms and surveillance equipment within the facility housing the information system or any information system components.

For enhancement PE-6(4), FIPS 199 High Impact systems must provide additional monitoring for those areas within facilities where there is a concentration of information system components (e.g., server rooms, media storage areas, communications centers) as approved by the AO.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.7 PE-8 Visitor Access Records

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides for [*GSA S/SO or Contractor recommended and AO approved time period*]; and
b. Reviews visitor access records [*at least annually*].

Control Enhancements: For high impact systems:

(1) Visitor Access Records | Automated Records Maintenance / Review. The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

GSA Implementation Guidance: Control PE-8 is applicable at all FIPS 199 levels. Enhancement PE-8(1) is applicable at the FIPS 199 High level.

GSA ensures maximum use of PIV and PIV technology, including PIV-I and CIV, to meet the objectives of CIO 2182.2. GSA records any temporary access to information systems with enough information to support an investigation, should evidence of a potential security breach occur. GSA reviews visitor access records annually in order to verify that GSA has effectively implemented and maintained proper visitor access procedures.

CIO 2100.1 requires visitor access records to include the following information:

- Name and Organization of the person visiting;
- Signature of the visitor;
- Form of identification;
- Date of access;
- Time of entry and departure;
- Purpose of visit;
- Name and organization of person visited; and
- Signature and name of individual verifying the visitor's credentials.

For enhancement PE-8(1), FIPS 199 High impact systems must implement automated mechanisms to assist in the review of visitor access records. Examples of mechanisms used to support the requirements of this enhancement would be reports generated from physical access control systems and visitor registration systems.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.8 PE-9 Power Equipment and Cabling

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

GSA Implementation Guidance: Control PE-9 is applicable at the FIPS 199 Moderate and High level.

GSA generally satisfies this control requirement through facility design requirements. GSA determines the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.9 PE-10 Emergency Shutoff

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
b. Places emergency shutoff switches or devices in [*GSA S/SO or Contractor recommended and AO approved location by information system or system component*] to facilitate safe and easy access for personnel; and
c. Protects emergency power shutoff capability from unauthorized activation.

GSA Implementation Guidance: Control PE-10 is applicable at the FIPS 199 Moderate and High level.

GSA facilities must have the ability to shut off power in the event of an emergency in areas with concentrations of information system resources such as, server rooms, tape libraries and data centers. GSA determines the need for emergency shutoff switches and devices as required per system requirements.

All personnel should be aware of emergency power shut off locations. Emergency shut off procedures must be documented. Emergency power shutoff capabilities must be protected from unauthorized activation.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.10 PE-11 Emergency Power

Control: The organization provides a short-term uninterruptible power supply to facilitate [*an orderly shutdown of the information system; transition of the information system to long-term alternate power*] in the event of a primary power source loss.

Control Enhancements:

(1) Emergency Power | Long-Term Alternate Power Supply - Minimal Operational Capability. The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

GSA Implementation Guidance: Control PE-11 is applicable at the FIPS 199 Moderate and High level. Enhancement PE-11(1) is applicable at the FIPS 199 High level.

GSA system documentation (e.g., SSP, Information System Contingency Plan) must clearly define the term of use for the uninterruptible power supply for moderate and high impact systems.

For enhancement PE-11(1), FIPS 199 High Impact systems must use a secondary commercial power supply or other external power supply. Long-term alternate power supplies for the information system can be either manually or automatically activated.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.11 PE-12 Emergency Lighting

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

GSA Implementation Guidance: Control PE-12 is applicable at all FIPS 199 levels.

GSA generally satisfies this control requirement through building design, existing building codes and regulations, and specifications included in contracts for facilities housing information systems. Each system security plan must describe how its facilities specifically meet this requirement.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.12 PE-13 Fire Protection

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Control Enhancements:

(1) Fire Protection | Detection Devices / Systems. The organization employs fire detection devices/systems for the information system that activate automatically and notify [*Information System Security Officer, System Owners, Acquisitions/Contracting Officers, Custodians*] and [*Police and Fire Department*] in the event of a fire.
(2) Fire Protection | Suppression Devices / Systems. The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to [*Information System Security Officer, System Owners, Acquisitions/Contracting Officers, Custodians,*] and [*Police and Fire Department*].
(3) Fire Protection | Automatic Fire Suppression. The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

GSA Implementation Guidance: Control PE-13 is applicable at all FIPS 199 levels. Enhancement PE-13(3) is applicable at the FIPS 199 Moderate and High level. Enhancement PE-13(1) and PE-13(2) are applicable at the FIPS 199 High level.

All FIPS 199 systems must ensure facilities containing concentrations of information system resources employ and maintain fire suppression and detection devices/systems for the resource(s) if supported by an independent energy source. GSA generally satisfies this control requirement through building design and existing codes and regulations. For moderate and high

impact systems, this control must be employed in facilities that are not staffed on a continuous basis. For all contractor and non-local personnel access, GSA ensures maximum use of PIV and PIV technology, including PIV-I and CIV, to meet the objectives of HSPD-12.

For enhancement PE-13(3), For FIPS 199 Moderate and High Impact systems, fire suppression and detection devices/systems must be automated.

For enhancements PE-13(1) and (2), FIPS 199 High Impact systems must utilize a notification list to identify specific personnel, roles, and emergency responders. Individuals on this list must have appropriate access authorizations and/or clearances in the event of an incident.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.13 PE-14 Temperature and Humidity Controls

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [*Data center temperature range (taken at the server inlets) should be 18 degrees Celsius to 27 degrees (64.4 degrees Fahrenheit to 80.6 degrees). Data center humidity levels (measured by dew point) should be within 5.5 degrees Celsius to 15 degrees (41.9 degrees Fahrenheit to 59 degrees). Ranges are consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) guidelines*]; and
b. Monitors temperature and humidity levels [*continuously*].

GSA Implementation Guidance: Control PE-14 is applicable at all FIPS 199 levels.

This control is implemented to protect the information system against damage or disruption caused by extreme temperatures or humidity levels.

GSA requires temperature and humidity levels to be consistent with ASHRAE guidelines: temperature for data centers (taken at the server inlets) between 18 - 27° C (64.4 – 80.6° F) and humidity levels, measured by dew point, between 5.5 - 15° C (41.9 - 59° F).

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.14 PE-15 Water Damage Protection

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Control Enhancements:

(1) Water Damage Protection | Automation Support. The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [*the Information System Security Officer, System Owners, and Custodians*].

GSA Implementation Guidance: Control PE-15 is applicable at all FIPS 199 levels. Enhancement PE-15(1) is applicable at the FIPS 199 High level.

For all FIPS 199 systems, water detection sensors, alarms, and notification systems must be installed and maintained within the facility housing the information system or any information system components. GSA generally satisfies this control requirement through building design and existing codes and regulations.

For enhancement PE-15(1), FIPS 199 High Impact systems water detection sensors, alarms, and notification systems must be automated.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.15 PE-16 Delivery and Removal

Control: The organization authorizes, monitors, and controls [*all information system components*] entering and exiting the facility and maintains records of those items.

GSA Implementation Guidance: Control PE-16 is applicable at all FIPS 199 levels.

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.16 PE-17 Alternate Work Site

Control: The organization:

a. Employs [*security control requirements as identified in GSA Order ADM 2450.1*] at alternate work sites;
b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

GSA Implementation Guidance: Control PE-17 is applicable at the FIPS 199 Moderate and High level.

Alternate work sites are sites that are geographically distinct from primary work sites. Alternate work sites may include government facilities or employee residences. Implement control requirements for alternate work sites IAW:

- GSA Order CIO 2104.1A, "*GSA Information Technology (IT) General Rules of Behavior*"
- GSA Order HCO 6040.1A, "*GSA Mobility and Telework Policy*"
- GSA Order ADM 2450.1, "*Alternate Sites for Continuity of Operations Plan (COOP) Relocation."*

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

3.17 PE-18 Location of Information System Components

Control: The organization positions information system components within the facility to minimize potential damage from [*GSA S/SO or Contractor and AO approved physical and environmental hazards*] and to minimize the opportunity for unauthorized access.

GSA Implementation Guidance: Control PE-18 is applicable at the FIPS 199 High level.

Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. The organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). GSA may satisfy this control by another organizational entity other than the information security program.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4 Physical and Environmental Protection and Supply Chain Risk Management

NIST SP 800-161 recommends Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) practices be used for FIPS 199 High systems. ICT SCRM processes increase the costs, both financial and time expended in supporting them, not just for GSA, but also for system integrators, suppliers, and service providers. ICT SCRM should be considered in the context of the system's missions, operational environments, and risks. Due to the increased costs involved in incorporating SCRM in physical and environmental protection processes the System Owner, IST Division Director, ISSM, and ISSO must carefully consider these costs prior to incorporating system specific SCRM processes into physical and environmental protection. Any questions regarding SCRM should be sent to ispcompliance@gsa.gov.

NIST SP 800-161 states, "*ICT supply chains span the physical and logical world. Physical factors include, for example, weather and road conditions that may have an impact to transporting ICT components (or devices) from one location to another between system integrators, suppliers, and organizations. If not properly addressed as a part of the ICT SCRM risk management processes, physical and environmental risks may have a negative impact on the organization's*

ability to receive critical components in a timely manner, which may in turn impact their ability to perform mission operations. Organizations should integrate physical and environmental protection controls into the ICT supply chain infrastructure to mitigate such risks and ensure that there are no gaps. It should be noted that the degree of physical and environmental protection required throughout the ICT supply chain is greatly dependent on the degree of integration between acquirer and system integrator/supplier/external service provider organizations, systems, and processes."

The PE controls addressed in NIST SP 800-161, limited to those controls for FIPS 199 High systems, are provided in the following sections along with NIST SP 800-161 supplemental guidance on the controls and GSA's implementation guidance.

4.1 PE-1 Physical and Environmental Protection Policy and Procedures (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: The organization should integrate ICT supply chain risks into physical and environmental protection policy and procedures. The degree of such protection required throughout the ICT supply chain is greatly dependent on the degree of integration between the organization and its system integrator, supplier, and external service provider systems and processes. The physical and environmental protection policy should ensure that the physical interfaces of the ICT supply chain infrastructure have adequate protection and audit for such protection.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must address physical and environmental risks associated with the ICT supply chain infrastructure. Depending upon the degree of integration between GSA and the system integrator, supplier, or external service provider of systems and processes these risks may be addressed by:

- Contract clauses
- Service Level Agreements
- Other methods approved by the GSA AO.

Audits of the protections called for by any of the methods identified above should be conducted to verify the protections are in place.

Additional Contractor System Considerations: *Contractor systems may defer to GSA policy and procedures as identified above or separately implement policy and procedures that facilitate the implementation of SCRM.*

4.2 PE-3 Physical Access Control (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Physical access control should include individuals and organizations engaged in the organization's ICT supply chain. A vetting process should be in place based on organizational-defined requirements and policy prior to granting access to the ICT supply chain infrastructure and any relevant elements. Access establishment, maintenance, and revocation processes should meet organizational access control policy rigor.

The speed of revocation for system integrators, external services providers, and suppliers needing access to physical facilities should be managed in accordance with the activities performed in their contracts. Prompt revocation is critical when either individual or organizational need no longer exists.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must verify that all personnel requiring access to facilities housing GSA information systems have been properly vetted IAW GSA Order ADM P 9732.1D, "*Suitability and Personnel Security*" prior to granting access to the ICT supply chain infrastructure and relevant elements of the system. Access establishment, maintenance, and revocation processes must meet the requirements for FIPS 199 High impact systems as established in PE-3.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.3 PE-6 Monitoring Physical Access (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Individuals physically accessing the organization's facilities, including the ICT supply chain infrastructure, may be employed by system integrators, suppliers, and external service providers. The organization should monitor these individuals' activities to reduce associated ICT supply chain risks.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must monitor the activities of individuals requiring access to GSA's ICT supply chain infrastructure, as established in PE-6. When escorts are required, the escort must be identified in the visitor access record IAW PE-8.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.4 PE-16 Delivery and Removal (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: This control enhancement reduces ICT supply chain risks introduced during the physical delivery and removal of hardware components from the organization's information systems or ICT supply chain infrastructure.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must authorize, monitor, and control all information system components entering and exiting the facility and maintain records of those items. Delivery and removal of hardware components must adhere to requirements established in PE-3 controlled IAW CIO-IT Security-01-05, "*Configuration Management*."

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.5 PE-17 Alternate Work Site (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: The organization should consider the ICT supply chain risks associated with organizational employees or system integrator personnel within or accessing the supply chain infrastructure using alternate work sites. This can include work from home or other non-work locations.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must ensure GSA Federal employees, contractors, and system integrator personnel within or accessing the supply chain infrastructure adhere to the requirements in PE-17.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.6 PE-18 Location of Information System Components (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Physical and environmental hazards have an impact on the availability of systems and components that are or will be acquired and physically transported to the organization's locations. For example, organizations should consider the location of information system components critical for agency operations when planning for alternative suppliers for these components.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM should consider physical and environmental hazards that affect the availability of information system components critical to agency as required in PE-18.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

5 Summary

GSA contractors and Federal employees should use this guide and the noted references to facilitate implementation of physical and environmental protection requirements. Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO ISP Division at ispcompliance@gsa.gov.